Rational Security: Modelling Everyday Password Use

Geoffrey B. Duggan, Hilary Johnson and Beate Grawemeyer

University of Bath
Bath, United Kingdom

Correspondence concerning this article should be sent to: Geoffrey Duggan, Department for Health, University of Bath, Bath, BA2 7AY, UK. Email: g.duggan@bath.ac.uk

Abstract

To inform the design of security policy, task models of password behaviour were constructed for different user groups – Computer Scientists, Administrative Staff and Students. These models identified internal and external constraints on user behaviour and the goals for password use within each group. Data were drawn from interviews and diaries of password use. Analyses indicated password security positively correlated with the sensitivity of the task, differences in frequency of password use were related to password security and patterns of password reuse were related to knowledge of security. Modelling revealed Computer Scientists viewed information security as part of their tasks and passwords provided a way of completing their work. By contrast, Admin and Student groups viewed passwords as a cost incurred when accessing the primary task. Differences between the models were related to differences in password security and used to suggest six recommendations for security officers to consider when setting password policy.

Keywords: Password, Security, Task Modeling, Rationality.

1. Introduction

The examination of security from an economic perspective has demonstrated that the structure of incentives for both users and companies can explain many shortcomings in security policy development and user behaviour (e.g. Anderson, 2001). Economic agents will only improve security when this leads either to some perceived benefit or reduction in cost. Security initiatives can fail not just through technical difficulties but also through insufficient incentives for those that implement the policy. Consequently, to understand the impact of a security policy not only do we need to understand the incentives that apply to an organisation but also the incentives that apply at the level of individual users. Further, we also need to understand the way that users react to incentives. One method to achieve this is to supplement economic arguments with a consideration of psychological factors. The current article takes a step in this direction by drawing on the psychological literature to model users' password security behaviour.

The importance of focusing upon the user's perspective has recently been illustrated by Herley (2009). He examined why user education has had limited effect upon the security of passwords, phishing site identification and SSL certificates. In short, the conclusion was that following much of the advice incurred considerable costs for the user while the benefits to the user were unclear or very small. For example, choosing long passwords that are not in the dictionary puts an additional memory load on the user but yields little benefit if accounts are locked out after a fixed number of failed logins. Further, even in instances (e.g. phishing) where the users' bank details could be compromised, the proportion of users actually affected is very small and banks typically reimburse customers who are victims of fraud. The point is that, given the costs and benefits, many of the decisions to ignore security guidelines are rational from the perspective of the user. This contrasts with the common assumption that a failure to comply with security guidelines is irrational.

Notwithstanding this analysis, there is however a large literature (see Kahneman, 2003) demonstrating that people are susceptible to a range of biases and their behaviour is not always consistent with the principles of normative rationality assumed within some economic models (e.g. Muth, 1961). Herley (2009) explained

that whilst security behaviour may be understood as rational, nonetheless, it is not clear that users will necessarily improve the security of their behaviour even where there are clear incentives. Spiekermann et al. (2001) compared self-reported privacy preferences of users with their actual self-disclosing behaviour during an online shopping episode. Most people stated that privacy was important to them and were particularly concerned about the disclosure of private information. However, even the most privacy conscious individuals, who presumably had a large incentive not to reveal such information, freely answered personal questions during the shopping task.

Apparent inconsistencies such as this and general biases in human behaviour can be explained as adaptations to limits imposed by time and by the external environment, along with the limited processing capability of the mind and competition between goals. These limits or *constraints* mean that the costs of calculating and following the optimal normative solution may not be justified by the benefits accrued. Thus, a more rational approach is to adopt alternative strategies that are adapted to the particular circumstances of the task, the environment and the individual (Anderson, 1990). In fact, following Howes et al. (2009), we argue that users are always rational insofar as they attempt to *maximize* "subjective expected utility" given the constraints on the cognitive architecture and the local task environment. This definition is an extension of "bounded rationality" (Simon, 1957) which suggests that people seek behaviours that are *sufficient* given the cognitive architecture and the local task environment.

Herley (2009) stresses the rationality of users' security behaviour by focusing on the *objective* costs and benefits for the individual user and illustrating the extent to which their behaviour is consistent with this objective evaluation. Because human cognition is extraordinarily adaptive (Anderson, 1990) we contend that maximizing subjective expected utility will often approximate behaviour based on an objective assessment of the costs and benefits. Where user security behaviour is not consistent with an objective cost-benefit assessment the discrepancy can be accounted for as error(s) in the users' judgements of subjective expected utility or as some constraint. Our approach is to identify these differences by drawing from the psychological literature and by building user and task models.

The security behaviour that we focus on is the creation and use of passwords on an everyday basis. Although alternative techniques such as graphical passwords (Wiedenbeck et al., 2005) and the use of passphrases (Keith et al., 2007) potentially offer more secure methods of authentication, passwords are still the most popular measure for protecting information. Despite this, or perhaps because of this, many problems with password usage and examples of bad security practice have been observed (Florencio and Herley, 2007; 2010; Schneier, 2000; Zviran and Haga, 1999).

Understanding the constraints that users operate under can help explain and/or help reduce the possible explanations for this bad practice. So, for example, limitations in memory capacity can constrain the length and number of passwords that users can remember (Vu et al., 2007). Similarly, an enforced security policy could provide a lower limit on the number of characters within a password or prevent the use of words from a dictionary. More subtly if, for example, users choose to write down a password rather than committing it to memory, then users must perceive the benefit for not having to remember a password to outweigh the possibility of, and costs associated with, an increased likelihood of a security breach. Perhaps because they consider it unlikely the service will be breached by someone reading the password, or perhaps a security breach will have little cost to the user. Of course, this may not reflect the actual costs and benefits for the user of writing down the password but it is the subjective judgement of the user that will determine their behaviour.

2. Related Approaches to Security

Some of the issues mentioned above have already been discussed within the context of the security domain. Most strikingly, in relation to privacy, Acquisti and Grossklags (2005) emphasized the importance of constraints and the need to consider rationality as bounded. They argued that although users reported growing concerns about privacy this did not necessarily translate into changes in behaviour. For example, 88% of people with high concerns about their name and address being stored in external databases still sign up for supermarket loyalty cards using their real identifying information. Acquisti and Grossklags contend that privacy decisions can be based on incomplete information and that decision making is subject to psychological constraints.

Our approach is aligned with Acquisti and Grossklags although, following Howes et al. (2009), we would also argue that within these constraints users are optimizers in that they will maximize subjective expected utility. More importantly though, the central aim of identifying and understanding constraints is common to both approaches. Here we address a different topic from privacy behaviour – the creation and use of passwords. Some constraints will be particular to the domain, most obviously those provided by the task and the environment. However, constraints related to the individual will also vary across contexts. For example, limitations in memory are probably more relevant to password use than privacy behaviour. In summary, this work extends many of the ideas from Acquisti and Grossklags to a different aspect of security behaviour and investigates the constraints within that particular domain.

Another relevant approach is the "Compliance Budget" (Beautement and Sasse, 2009). This emphasizes the importance of understanding the costs and benefits for the individual user and states that compliance occurs when the cost-benefit outcome of following a policy is greater than the cost-benefit outcome of not following it. Beautement and Sasse (2009) argue that the amount of effort users are prepared to expend on compliance is limited and that it is difficult to get users to comply with security policy once this budget is exceeded. We suggest that *any* effort expended on compliance must accrue some benefit that outweighs the costs in terms of subjective expected utility. However, this observation only has value insomuch as it leads to explanations of *why* users expend "compliance effort". This paper models the specific case for password use but, in the general case, we speculate that some benefits for compliance effort could be perceptions of increased self-worth, avoidance of punishments for security breaches or the reduction of worry that a security breach will occur.

Beautement and Sasse (2009) stress that the compliance budget is limited and, over time, users are increasingly less likely to follow additional security policies that require "compliance effort". There are a number of potential explanations for this. Firstly, the cost of each additional security policy could be additive, thus increasing the overall cost and the extent to which other activities are compromised. Secondly,

the benefits associated with compliance may well be subject to diminishing marginal returns. For example, any increase in self-worth is unlikely to be directly proportional to the number of policies followed. Thirdly, each additional policy may also be perceived as predictive that there will be further future policies to follow. Fourthly, users may initially be more likely to explore or try new behaviours (i.e. complying with a guideline), as any possible benefit from the new behaviour can be enjoyed for longer. However, over time, the reward from exploring is reduced as at some point the user must focus on exploiting the current behaviours (Cohen et al., 2007).

Cranor (2008) describes a system for reasoning about the human in the loop within secure systems. She developed her framework from the Communication-Human Information Processing model from the literature related to warnings (Wogalter, 2006). Applying this framework to passwords led Cranor to the conclusion that the most critical failure is a failure in the capabilities of users, that is, people are not capable of remembering large numbers of policy-compliant passwords. However, the memory literature indicates that humans are capable of remembering vast amounts of information (Ericsson and Polson, 1988) and with sufficient rehearsal large numbers of passwords could potentially be remembered. Our approach stresses the judgement users make about the costs of correctly remembering large numbers of passwords (primarily time spent rehearsing) relative to the benefits accrued. Memory constraints are typically not an all-or-none capability and instead will predict the likelihood of failure given time spent rehearsing. (See also Komanduri et al., 2011, for evidence of the complex strategies users apply during password composition, presumably to accommodate different memory constraints.) We shall expand Cranor's conclusion that memory constraints can affect password use by identifying characteristics of memory from the literature and predicting their effect on password use.

3. Constraints on Password Security

3.1. Memory Constraints

Ultimately, the effectiveness of the password as a security tool is dependent on the ability of the user to remember it and any failure to remember a password will increase the cost to the user of following the security policy. This cost could include

the set up costs of creating a new password, the social embarrassment of explaining the password has been forgotten and the delay or even failure to complete the task for which the password was required. These costs mean that users need to choose passwords that best exploit their memory resources.

Two of the most basic findings from the memory literature are that recall for an item is related to the frequency with which it has been recalled and the time since it was last recalled (Ebbinghaus, 1885, 1964). More elaborately, Anderson and Schooler (1991) demonstrate that power functions describe both the rate of forgetting between presentation and test, and the improvement in learning due to practice. Therefore, passwords will be more easily recalled when they have been used recently and frequently. In everyday life, the frequency with which a password is used is determined by the number of times the user wants to access the password-controlled service or task. Nevertheless, because users choose which passwords are used for which tasks, they could adapt their choice of password to exploit the ease of recall for frequent and recent information.

Our approach predicts that users will adapt their strategies to the local task environment (Anderson, 1990). Thus, if passwords that are rarely used are harder to remember then users are likely to adopt strategies that support the recall of infrequently used passwords. Similarly, there will be less need to adopt such strategies for frequently used passwords. Example strategies that would increase the memorability of a password are reusing the password for more than one service, writing down the password, constructing a password more closely related to the particular service (e.g. using “worklogin” as a password to login to an account at work) or constructing a password using a memorable word from the dictionary. All of these strategies reduce the security of the password, but as the difficulty of remembering the password increases, it becomes more costly for the user to maintain high levels of security. Therefore, we predict that users will rationally adapt to differences in frequency of password use and exploit these strategies for less frequently used passwords, resulting in less secure passwords. More secure passwords will be constructed for more frequently accessed services. Because users are maximizing *subjective* expected utility, we assess this prediction using participants’ estimates of password security rather than an objective measure of password security.

3.2. Knowledge Constraints

Another potential constraint upon the security of passwords is the users' knowledge of security appropriate behaviour. Users must be aware of a security procedure before they can use it to inform the construction of passwords. Set against the value of security knowledge, is the cost in terms of time and effort required to find and understand guidelines for the construction and use of passwords. Even if this cost is worthwhile, there are a whole range of different guidelines for password construction available, some of which contradict each other, meaning that the potential benefits from finding information about secure password use are unclear (Herley, 2009). More generally, determining the appropriate amount of information to acquire before decision-making is a difficult problem to resolve (Browne and Pitts, 2004). These factors mean that there are likely to be gaps in users' knowledge about password security and there is evidence for this within the security literature (Hoonakker et al., 2009; Sasse et al., 2001; Zviran and Haga, 1999).

These gaps in security knowledge can directly affect behaviour, for example, Jensen et al. (2005) found that limitations in the understanding of privacy technology affected users' behaviour online. In our study, we chose to investigate the extent to which differences in security knowledge affect the *reuse* of passwords. Reusing passwords for more than one account is a commonly reported strategy for reducing memory load that can compromise security (Florencio and Herley, 2007; Ives et al., 2004; Shay et al., 2010). However, survey data from Gaw and Felten (2006) indicate that users are not always clear about the consequences of password reuse for password security. If there are differences in security knowledge then this could affect the overall level of password reuse and also the type of accounts for which passwords are shared. A rational account predicts that a greater awareness of the security consequences of password reuse will reduce the overall level of reuse and mean that users are less likely to reuse passwords for more sensitive services.

3.3. Comparisons Between Groups of Users

To investigate the constraints that affect password use, we conducted a diary study of everyday password use. Grawemeyer and Johnson (2011) in a study concerned with the management of multiple passwords, report descriptive statistics from this study examining password use over the study period and the activities that required password activation in a typical day. They found that users often violated security guidelines and that many of these problems arose from the difficulty of managing a whole collection of passwords.

In drawing conclusions about password use and misuse from the diary study sample, Grawemeyer and Johnson (2011) treated the users as a single group and did not focus upon individual differences between users. However, the users originated from three different job roles and here we exploit these real world differences to speculate about variations in password use. Security policies will often incorporate employees with different job roles and different user characteristics. Studying between-group differences in security behaviour enables policies to be developed that can be applied across different user groups or, where this is not possible, to suggest ways that a policy must be adapted according to the particular group or task.

Furthermore, because the groups were relatively homogenous we can identify factors that may differ systematically between groups and could be subjected to further study using larger populations. Because these groups reflect real world distinctions any differences are likely to have greater applicability to other contexts of password use. Shay et al. (2010) gathered survey data on password use by faculty members and students and found the groups varied across a number of dimensions including instances of forgetting and strategies for remembering passwords.

The three groups of users in this study were Students, Administrative Staff and Computer Scientists. These groups reflect differences in security knowledge and are representative of different groups that use passwords. We present tests of the predictions relating to memory, security knowledge and task structure for each of our user groups. These data along with interviews with members from each group were then used to build task models with the active involvement of users, describing password behaviour in each of the groups. These models are presented in Section 6

and are an attempt to characterize the key constraints that affect password behaviour in different groups of users.

4. Method

Our approach was to combine a diary study of password authentications with a debrief interview for each password used. In addition, one randomly selected participant from each group individually collaborated with model building. This combination of methods enabled detailed recording of *in situ* behaviour along with a more elaborate understanding of the individual passwords themselves and the rationale behind their selection. The diaries were used both to provide information about participant behaviour and as a prompt for the debrief interviews around each password (Carter & Mankoff, 2005).

The sample size of the dataset was not large (22 participants) but our approach employed multiple data gathering phases that yielded large amounts of quantitative (991 separate password authentications) and qualitative data (25 separate interviews). The decision to trade-off breadth of sample size for depth of detail was made with a view to maximizing the sophistication of the models of password behaviour in Section 6. This design strategy is not unusual within modelling approaches (e.g. Johnson and Hyde, 2003; Fischer, 2001) and complements the data gathering with vast numbers of participants that has already taken place within the password literature (e.g. Florencio and Herley, 2007, Bonneau and Preibusch, 2010).

4.1. Participants

Participants were recruited from a commercial technology organization (HP Labs) and a research intensive university (University of Bath). The study was conducted at the start of 2009 and participants received a £20 book token as compensation for their time. The three groups of participants were:
Administrative staff. All 6 were female and worked in office administration roles providing support for non-security based tasks, 2 were educated in IT. One was in the age range 20-29, 2 in the age range 30-39, and 3 between 40 and 49 years.

Computer Scientists. Six computer scientists (2 female) working as either system engineers or researchers, all had an educational background in IT. One was in the age range 20-29, 2 in the age range 30-39, and 3 between 40 and 49 years.
Students. Ten students (4 female) from a variety of educational backgrounds. Six were in the age range 20-29, 2 between 30-39, and 2 between 40-49 years of age

4.2. Materials

The diary consisted of a form that required information about the authentication process to be entered into boxes. In the order on which they were presented on the form the items were: the time of authentication; which password was used (the actual password was not divulged); location (home, office, mobile or other); activity before and after authentication; whether any hints were provided; the estimated time taken to authenticate; whether the authentication was successful or failed; if it failed, what the nature of the problem was for example, whether the participant knew if the failure originated from either mistyping (a typographical error) or misremembering, and what participants did in order to recover from failure (for example, try again or call the helpdesk).

For the debrief interview a form was used to structure the interview around each password. This form assessed perceived sensitivity of the task accessed and the user's estimate of the security of the password using 5 point Likert-style scales ranging from "very sensitive" to "not at all sensitive" for perceived task sensitivity and from "highly secure (uncrackable)" to "insecure (easy to guess)" for estimated security. It was important to collect *subjective* estimates of task sensitivity and password security as cognitively bounded rationality assumes users maximize *subjective* expected utility. The structure of the passwords was recorded by the participants themselves categorizing passwords, with respect to individual features such as length, inclusion of letters/digits/non-alphanumeric characters and whether the password included a word or common name. Also included were questions about how participants remembered the password and whether it was reused to access other services.

4.3. Procedure

The diary study was conducted over a seven-day period in line with the recommendations of Rieman (1993). Throughout that time participants were required to go about their routine as normal and record in the diary every instance during the day or evening when they entered a password. Participants were instructed not to reveal their actual passwords at any point during the study. The aims of the study were explained including the purpose of maintaining the diary.

Upon completion of the diary period a structured interview based around the debrief form was conducted. A separate form was completed for every password used during the diary period to ensure that all the password types were discussed fully. As well as the structured questions, participants were encouraged to expand upon their responses and elaborate upon any points arising from the diary entries. Prior to completing the diary participants were made aware that there would be a subsequent debrief interview to gather additional information about the characteristics of the passwords used, but not the actual passwords themselves.

As well as the quantitative data arising from specific questions the debrief interviews provided rich qualitative data for each password used during the diary period. These data were expanded upon in a second modelling session with one representative chosen at random from each group. More detail about the modelling process is given in Section 6.1.

5. Results

The focus of our analyses and subsequent modelling was to develop an understanding of password security in each of the three groups. Therefore, unless otherwise stated, all analyses were conducted separately for each group. As in Inglesant and Sasse (2010), analyses focused on the password as the object of study. Passwords that were used by the same participant for more than one service were only included once in the dataset. There were 42 passwords in the Computer Scientist group, 74 passwords in the Student group and 38 passwords in the Admin group.

All participants made diary entries across the whole period of the study and during the debrief interviews reported that, as far as they were aware, they had remembered to

record instances of password entry during the study period and that these recordings were made immediately after entering a password.

5.1. Types of passwords created

Firstly we describe the different types of passwords created. Each password was assigned to one of the following categories, i) single word or name (e.g. 'Lucy'); ii) meaningful phrase (a simple sentence where the words are connected, e.g. 'WhoHasSentMeNewMail'); iii) abbreviation of a meaningful phrase (the initial letters of a sentence, e.g. the first letters of the sentence 'Who has sent me new mail?' would be `Whsmnm?'); iv) a meaningful combination of letters and numbers (e.g. initials and birthdays); v) a meaningful number pattern (e.g. '0845'); vi) random characters; or vii) some other pattern (a combination of e.g. words and letters).

Table 1 shows the proportion of passwords in each group that fell into each of these categories. The distribution of proportions across categories varies greatly between the three groups. For example, the most common category of password is different in each of the groups. Also striking is that the proportion of passwords that were single words or names, was much higher in the Admin group. These passwords are more vulnerable to attack than less predictable character strings (Yan et al., 2004). In sum, these data suggest that the groups differ in the passwords they create and that these differences have implications for security.

5.2. Estimated password security and perceived task sensitivity

The data in Table 1 show that users do not select the most secure passwords possible for all services. Our rational approach assumes this is due to constraints relating to the user and the environment. To use this rational approach to help identify these constraints we must first establish whether users adapt the security of their password to the sensitivity of the service being accessed.

Figure 1 shows the correlation between perceived task sensitivity and estimated security in each of the three user groups. The figure indicates that in all three groups the estimated security increased as the rated task sensitivity increased. Spearman's ρ

correlations found this effect was reliable in all three groups: Computer Scientist, $\rho(42) = .56$, $p < .001$; Student, $\rho(74) = .36$, $p = .002$; Admin, $\rho(38) = .50$, $p = .002$. These correlations are relatively high particularly as they do not account for any other factors that might influence behaviour. This suggests that all three groups adapted their selection of passwords to the sensitivity of the task and that to some extent users are motivated by security considerations.

The correlations are, however, far from perfect in all three groups and in particular for the Student group. Thus, there are other constraints influencing password use that are not accounted for in this simple analysis. The remainder of this section will be spent trying to identify and understand these constraints.

One constraint that could explain the correlations is the password requirements that are enforced by the system. The correlations could simply reflect a tendency for more sensitive services to have stricter security policies. To address this, any passwords where participants reported a system-enforced policy were removed from the analysis (28%). This alteration did not change the pattern of results or statistical significance and the size of the correlation remained approximately the same in all three groups.

5.3. Frequency of password use

The literature on memory indicated that users will find it easier to recall passwords when they are used frequently. We predicted that, for more frequently used passwords, participants would be less likely to use strategies that aid recall but compromise security. Therefore, estimated security should be positively correlated with the frequency of password usage. The advantage for adapting strategy across passwords is dependent on the variance in frequency of password use. For groups with large differences in the frequency with which passwords are used there will be a greater advantage for adapting to the environment.

The frequency with which passwords were used during the diary period was higher in the Computer Scientist group ($M = 9.83$, $SD = 17.98$) than in the Student group ($M = 4.55$, $SD = 4.97$) and the Admin group ($M = 5.08$, $SD = 6.21$). A one way ANOVA between participants across all groups found this difference was significant, $F(2, 151)$

= 3.67, p = .03. Importantly, the variance in frequency of use was different between the three groups. The standard deviation was much higher in the Computer Scientist group indicating there was greater opportunity for that group to adapt the security of their passwords to the frequency of usage.

The prediction that participants would find frequently used passwords easier to recall was supported by the data. Across all groups, participants reported that passwords used 10 times or more during the study were recalled "automatically" 83% of the time, whereas passwords used fewer than 10 times were recalled automatically 50% of the time. This difference between the groups was significant, χ^2 (153) = 9.31, p = .002. The extent to which each group exploited this ease of recall for high frequency passwords was tested using a Spearman's ρ correlation between estimated security and frequency of use.

Figure 2 shows there was a significant positive correlation in the Computer Scientist group meaning that frequently used passwords had higher estimated security, $\rho(42)$ = .30, p = .05. The figure also shows there was no clear relationship between frequency of use and estimated security in both the Student group, $\rho(74)$ = -.12, and the Admin group, $\rho(38)$ = -.08. These results suggest that participants adapted their password security in response to the structure of the task environment. In both the Student and Admin groups frequency of use did not vary greatly between passwords meaning there was little scope for improving the security of frequently used passwords. In contrast, there was greater variation in frequency of password use in the Computer Scientist group and these participants appeared to exploit this and construct more secure passwords for more frequently accessed services.

5.4. Password Reuse

The proportion of passwords that participants reported were reused for other accounts differed between the 3 groups. There were fewer passwords reused in the Computer Scientist group (43%) than in the Student group (64%) or the Admin group (68%). Chi-square analysis compared the total number of passwords that were reused or unique in each group and this found a significant difference between the groups, $\chi^2(2)$

= 6.55, p = .04. Passwords that reused only part of another password were treated as unique.

One explanation for the difference in reuse between groups was that they reflected differences in knowledge of security procedures. This explanation was tested by comparing perceived task sensitivity for unique and reused passwords. A rational account predicts that an increased awareness of the negative consequences of reuse for security would lead participants to restrict reuse to passwords that provide access to less sensitive services. Therefore, we predict that in the Computer Scientist group perceived task sensitivity should be lower for reused passwords than for unique passwords. If the higher levels of reuse found in the Student and Admin groups were due to lower knowledge about factors that affect security, then we predict that these groups will be less likely to concentrate reuse upon less sensitive tasks. Therefore, for the Student and Admin groups there should be no difference or a small difference in the perceived task sensitivity for reused passwords and unique passwords.

Figure 3 shows the mean perceived task sensitivity and standard error for unique passwords and reused passwords in each of the three groups. Mann-Whitney U tests compared the task sensitivity for unique and reused passwords within each of the three groups. Perceived task sensitivity was higher for unique passwords than for reused passwords in the Computer Scientist group, $U(42) = 92.50$, $Z = -3.27$, $p = .001$. There was no difference in perceived task sensitivity for unique and reused passwords in the Student group, $U(74) = 600.50$, $Z = -.40$, $p = .69$, or the Admin group, $U(38) = 155.50$, $Z = -.02$, $p = .99$. Therefore, the Computer Scientists appeared to adapt their password reuse to the security risk – more sensitive services were more likely to be accessed with a unique password. By reusing passwords for less sensitive tasks the Computer Scientist group *lessened the number of passwords that had to be remembered without increasing the security risk to the most sensitive tasks.*

Password reuse is one means of increasing the memorability of a password at the expense of security, therefore, reuse could be an adaptation to the frequency with which a password is used. This test of adaptation to frequency is not as strong as the correlation in Figure 2 because password reuse is only one of a number of strategies that could be used to trade-off security with memorability. Nonetheless, given that

reuse appeared to be adapted to the sensitivity of the task in the Computer Scientist group, it is interesting to compare the frequency of usage for reused passwords and for unique passwords. Because frequency of password use varied more in the Computer Scientist group and because security was better in the Computer Scientist group we would expect a greater difference in frequency of usage in the Computer Scientist group than in the Student or Admin groups.

The means and standard errors for frequency of use for unique and reused passwords in each group are given in Figure 4. Mann-Whitney *U* tests compared task frequency for unique and reused passwords in each of the three groups. As predicted, in the Computer Scientist group unique passwords were used more frequently than reused passwords, but this difference was not reliable, U (42) = 187, Z = -.76, p = .45. For the Student and Admin groups, average usage of reused passwords was higher than for unique passwords. This difference was significant in the Student group, U (74) = 447, Z = -2.16, p = .03, but was not significant in the Admin group, U (38) = 106.50, Z = -1.58, p = .12. Thus, there was some indication that the differences between groups in the frequency of password use may affect the pattern of reuse. That is, passwords that were frequently used were less likely to be reused in the Computer Scientist group which may have contributed to the lower overall levels of reuse in the Computer Scientist group. Although it should be stressed this result was not significant.

The significantly higher frequency of use for reused passwords in the Student group indicates that some other constraint was influencing their behaviour. Also, the correlation in Figure 1 was smaller in the Student group than in the Computer Scientist or Admin groups. A speculative explanation for this pattern is that motivation towards security was lower in the Student group. This result and the general attempt to understand the relationship between reuse and task frequency illustrate the way that more complicated models of user security behaviour can be developed by considering multiple constraints in combination.

6. Task Modelling

Having tested our hypotheses regarding password reuse and frequency of password use, we now seek to use these analyses along with the data from the diary study and the debrief interviews to construct models of password behaviour in each of the three groups. The general purpose of such modelling is to create an abstraction that succinctly describes the phenomena of interest. Such a representation enables the identification of relevant factors that determine behaviour, and crucially, enhances understanding of this behaviour. Making sense of behaviour in a format other than textual description supports comparison across models, the identification of strengths and weaknesses and highlights the absence of particular factors within a model.

Models of users have been widely used within Human-Computer Interaction and task models have been used for training purposes and for generating and evaluating interface designs to support task behaviour (Allen, 1990; Johnson and Johnson, 1989; McCrickard et al., 2003). Therefore, this approach seems applicable to understanding enabling security tasks such as password creation, use and misuse. This will enable us to assess and outline clearly the different constraints that each individual user or user group is operating under. Further, the process of constructing the models should generate reflection from the user groups about their behaviour and perhaps lead to initial suggestions about how to change behaviour. For example, should specific constraints be relaxed or even removed and if so which constraints?

During password creation and use, the user has a large amount of discretion over how they complete the task meaning that internal constraints are likely to be an important component of variance in behaviour between participants and groups. These internal constraints include knowledge of security policies and likelihood of threats as well as user motivation. Further internal constraints are knowledge about the task itself and the relative security of different types of password. Users must devise strategies for creating and maintaining passwords within these constraints, therefore knowledge of strategies is another important internal constraint. Table 2 provides a list of some internal constraints that affect password behaviour.

There are also external constraints that can affect password behaviour. Table 3 shows external constraints grouped by the organization, the environment and the task. Some of these constraints are likely to be more or less important across the three different

groups. Our models will attempt to capture the way that users adapt to these differences in external constraints and the implications for password behaviour.

The way that users respond to the constraints in Tables 2 and 3 will be determined by their knowledge of them and their knowledge of strategies for adapting to them. Therefore, our modelling approach is to represent password behaviour in terms of Task Knowledge Structures. An advantage of this approach is that, as well as representing the task itself, a TKS can show the underlying knowledge (or lack of knowledge) that each participant or group may have. Because users have a considerable discretion over their password behaviour we believe that differences in knowledge are likely to be an important determinant of any differences in password security. Although TKS has been successfully applied to user behaviour across a range of contexts (Johnson and Hyde, 2003; O'Neill et al., 1999; Wild et al., 2004), it has not been used within the security domain. Thus, a secondary aim for the modelling is to further develop the approach in the light of the data relating to passwords.

6.1. Construction of TKS Models

The construction of TKS models requires specific types of data about goals, objects, actions, procedures as object-action pairings, strategies etc. To extract this information specific questions were included within the debrief interview. For example, participants were asked how passwords were created, what procedures were followed and how passwords were passwords. These data from the debrief interview were combined with password diary data and used as the basis for the modelling. To check that these data sources were sufficient to construct TKS models and to test if anything was missing we conducted a second session with one participant from each group.

During the second session, the researcher and the participant collaboratively constructed models of password creation and usage for that individual and for their group. Including the representation as part of the session encouraged reflection by the participants and also reduced the likelihood of inaccuracy and misinterpretation by the researcher. This second session lasted approximately an hour and included a number

of methods to aid model construction. For example, objects, actions and procedures from the diary and debrief were provided on separate pieces of paper and participants were asked to show how they were used. This was used to clarify aspects of the model such as which actions and objects were paired together (e.g. were passwords with symbols in them likely to be forgotten), which procedures were followed (e.g. was the likelihood of a security breach ever considered) and in what order were procedures completed (e.g. was the required password length checked before attempting to create a password).

Participants were also asked to construct a goal structure to describe their behaviour and discuss any associated trade-offs between security and other priorities. Wherever possible participants were encouraged to construct the model on their own and volunteer information. When they were unable to do this the researcher assisted with prompts for more information or questions about the relationships between different aspects of the model.

After constructing a TKS that described their own password behaviour, participants were then asked to construct a representative or composite TKS for their group (i.e. Admin, Computer Scientist or Student) and to comment on which elements from their own model would generalize to the group as a whole and any other factors that needed to be added or taken away. The models constructed during the session included a skeleton structure and the composite model for each group, which were constructed by adding information from the diary study and debrief interviews. Elements were only added to the composite model when they were reported by more than one member of the group or were deemed as representative of the group during an interview.

There was no hard evidence for post hoc rationalizing of security behaviour during the interview. To minimize the likelihood of this it was emphasized to participants that we were interested in their actual security behaviour and reasoning rather than what they were “supposed to do”. During the interview comments and justifications were tied back to other aspects of their dataset to verify the reasoning reported and any apparent discrepancies were discussed. However, such discrepancies were unusual.

6.2. Admin TKS

To illustrate the process of constructing TKS models for each of the groups we shall include the initial model constructed for a single participant from the Admin group before describing the composite model for the whole group. The TKS for the individual participant is given in Figure 5. A strong theme that emerged from the modelling was a clear separation between work and leisure. The participant had quite distinct strategies for each situation "… that's only for my passwords at home. I'd never do that in work."

The participant considered work passwords were more likely to be attacked than leisure passwords and that a security breach at work would have serious consequences both for themselves and the organization. Accordingly, at work they used a password that they believed was less memorable but harder to guess/crack. This password was also not shared with anyone or written down. By contrast, almost all non-work activities were considered relatively low risk and the participant judged the passwords used for these activities to be more guessable and shared them in part or whole with other family members. Outside of work, no adjustment was made for any services perceived as less secure where passwords might be compromised.

This participant also reused passwords extensively but kept the distinction between work and leisure tasks. All work tasks were completed using the same password but this password was never used for non-work tasks. They reported that this reuse was partially due to the frequency with which they had to interleave between tasks that required passwords. "I'm always jumping between one thing and another so it's easier to just have the same password that I can keep using each time." A password was chosen at random from three other passwords for almost all leisure tasks. These three passwords all contained the same stem.

The participant was concerned about security at work and aware of some security guidelines – for example: "I have numbers as well as letters which makes it more difficult to guess". Nonetheless, there were gaps in knowledge and limits in the extent to which guidelines were applied: "I never actually change it [a password used at

work] because I might not be able to remember the new one and I don't want to have to go and explain I've forgotten it." Ultimately, the participant was prepared to incur some cost at work as they perceived security to be important but they were not prepared to implement security guidelines when the cost interfered with their productivity at work. Outside of work the priority was to minimize the inconvenience of remembering passwords rather than the security of the services being accessed.

To create a composite TKS for the whole Admin group we returned to the debrief and diary data and integrated that information with the individual TKS from Figure 5. This composite TKS is given in Figure 6, it shows that other group members had a strategy of using short passwords wherever possible and only extending them when the system required this. There was also sharing of passwords with colleagues as well as family members and a lower awareness of security guidelines by the group as a whole than for the individual who took part in the modelling session. Although the distinction between work and leisure was relevant to most group members, there was not the same clear divide in strategies applied and some passwords were reused across both contexts. Finally, other group members emphasized that the task environment included external interruptions and forced switches between tasks.

6.3. Student TKS

For brevity only the composite models are presented for the Student and Computer Scientist groups, the TKS for the Student group is given in Figure 7. There are a number of elements in common with the Admin group particularly within the strategies employed. Students also frequently reused passwords across services and did not change their password very often. However, there were also clear differences between the groups.

Firstly, the distinction between work and leisure was not particularly relevant to most students and they freely shared passwords across services and did not adopt different strategies for password creation for work or non-work tasks. This is perhaps unsurprising given the students were not actually employed by any organization, nevertheless, it is interesting to model behaviour when there is little responsibility to any external organization. The interviews found that many students perceived their

passwords to be under little risk of attack and that this decreased their willingness to create and maintain secure passwords.

Another clear trend was that the students were on average more knowledgeable about security guidelines and procedures than members of the Admin group. Some not only understood password guidelines but were also aware of shortcomings with the guidelines and actively adjusted their behaviour on this basis. For example, one group member said "I'd never put anything really valuable online because you'll never be able to stop someone hacking my computer and getting my password through keylogging".

Other noteworthy details from Figure 7 are the high degree of discretion over task interleaving (Payne et al., 2007). Participants were often able to choose what they worked on when and were not forced to frequently jump between password protected services. There was also a greater emphasis placed upon protecting privacy by this group "what I'd be really bothered about is if someone could access my Facebook account not work stuff." Many of the services rated most sensitive were social networking sites. This may reflect a greater tendency to share more information online than a greater concern with privacy.

6.4. Computer Scientist TKS

The model for the Computer Scientist group in Figure 8 shows that this group were very knowledgeable about security guidelines for passwords. Interestingly, given their interest in computer science some group members chose to stay abreast of developments in password security as part of their job. "I usually know what's going on in security because I'm interested in it anyway and I get sent updates and information all the time." This also seemed to change their perception of the security task. Rather than viewing password protection as a cost that had to be borne, they viewed passwords as an asset – a way of protecting their information. "The important thing is that my stuff is safe. I want to have control over that." and "Not having strong passwords is just stupid, they mean that I can do what I want. [That] I can do my job basically."

The model also shows that the Computer Scientists were motivated to create secure passwords and, relative to the other groups, they believed there was a higher risk of a security breach and that this would have more serious consequences. This high knowledge about password security and high motivation translated into more sophisticated strategies being used for password generation for the sensitive services. Some participants applied these strategies across all passwords, however, hard-to-remember passwords were typically only generated for the most sensitive services.

There was also a high frequency of task interleaving in the Computer Scientist group. Some of this was under the participants' control but the structure of the job also forced participants to enter some passwords frequently. Although passwords were reused across non-sensitive services, typically only part of a password was reused.

6.5. Conclusions from modelling

The goals for password behaviour differed importantly between the three groups. The models reflect differences in the importance attached to password security between groups. They also reflect differences in the way the goals were expressed and we argue that these differences in emphasis can have consequences for password behaviour.

More specifically, the Computer Scientist group appeared to view security as part of the task they were completing. Thus, passwords enabled them to protect their work and thus complete their tasks. Accordingly, the benefits for secure passwords were most salient to this group and they were motivated to create passwords that minimized the likelihood of a security breach. In contrast, the Admin and Student groups viewed passwords as simply a cost that was incurred when completing their primary task. Therefore, many of their passwords were chosen to minimize the cost of remembering rather than for security reasons. Where these participants considered security to be part of their job role (i.e. for the Admin group at work), then more secure passwords were constructed.

Knowledge about password guidelines and security in general also differed between the three groups. The Computer Scientist group was the most knowledgeable

followed by the Student group and then the Admin group. The Computer Scientist group was also more likely to follow these guidelines and their password behaviour was most consistent with security recommendations. Interestingly, although the Admin group had the lowest security knowledge their work passwords were typically more secure than passwords in the Student group. Thus, security knowledge appeared to be an important factor in password security but it interacted with other variables such as motivation.

The analyses in Section 5.4 found that in the Student and Admin groups password reuse was commonplace and this included passwords for sensitive services. The modelling process revealed that these groups were aware of the potential vulnerability caused by a compromised password that had been reused. However, the modelling also indicated that group members felt that most, if not all, of their accounts were at very low risk of being attacked. That is, although they often cared that the information was not accessed by others, they believed that this was unlikely so did not invest effort in creating and maintaining unique passwords. In general, the Computer Scientists believed there was a higher risk of accounts being compromised and were less prepared to reuse passwords for sensitive services.

7. Discussion

7.1. Summary

A key idea underpinning this work is that users are rational – they maximize subjective expected utility (Howes et al., 2009). Given this premise, we tested the importance of password security to users by examining whether they adjusted the security of their passwords to the sensitivity of the service being accessed. Across three different groups of users, we found that password security correlated with the sensitivity of the service. These correlations also indicated that there were factors, or constraints, other than security that affected password behaviour. Further, the results showed differences between groups in the types of passwords used. Our aim was to identify these constraints for each of the user groups by drawing on the psychological literature and constructing task models.

The literature on memory led to the prediction that users would adapt to large differences in frequency of password use by constructing more secure passwords for more frequently accessed services. Within the Computer Scientist group there was high variance in frequency of password use and a positive correlation between frequency of use and estimated security. By contrast, frequency of use did not vary greatly between passwords in the Student and Admin groups and did not correlate with estimated security.

Another potential constraint on password behaviour is task knowledge. We predicted that groups that were more knowledgeable about password security would reduce password reuse for more sensitive tasks relative to less sensitive tasks. This prediction was supported as perceived task sensitivity was higher for unique passwords than for reused passwords in the Computer Scientist group and there was no difference in perceived task sensitivity for unique and reused passwords in the Student and Admin groups.

To better understand password behaviour we modeled each of the three groups, this process identified differences in task knowledge, procedures and strategies. These models also revealed the groups had different goals when creating and using passwords. The Computer Scientists viewed information security as part of their tasks and passwords provided a way of completing their work. By contrast, the Admin and Student groups viewed passwords as a cost incurred when accessing the primary task. For the Computer Scientist group increasing password security led to large gains in subjective expected utility, whereas for the Admin and Student groups minimizing the cost of remembering a password led to larger gains in subjective expected utility. Therefore, our data clearly illustrate the value in understanding both the constraints that each user or group operate under as well the goal(s) that they are trying to achieve.

7.2. Applications to Security Policy

Unsurprisingly, the models in Section 6 show that everyday password use is affected by a range of factors that interact in complex ways. To account for this complexity we avoid rigid recommendations that will not hold in many instances. Instead, following

Pawson and Tilley (1997), we point to key relationships between factors and their implications for password security. The aim is to support the expert security officer who can then apply those recommendations that are pertinent to their particular circumstances. Encouraging security officers to account for a large range of variables is likely to increase the complexity of their decisions. However, we hope that this could be offset by advances in decision support systems developed for security officers (e.g. Baldwin et al., 2011, Parkin et al., 2010). Recommendations:

1. Account for users' job roles. Both the quantitative results and the modelling demonstrated different approaches to password security from users with different job roles. Specific factors are considered in recommendations 2-6, but our results make the general point that different groups of users are likely to respond differently to security policies and that job role can predict some of this variance. Tailoring password policies to specific groups may not always be practical and where security officers are constructing a policy that will cut across many different job roles our results indicate they should set policy for the least security conscious groups. Otherwise, users may adopt nonsecure workarounds such as reuse and writing passwords down (see Figures 6 and 7).

2. Adapt security policy to frequency of password use. For passwords used relatively frequently, users' memory was more automatic and more secure passwords were constructed. Thus, users will find it easier to comply with stricter password policies for services that are accessed very frequently.

3. Adapt security policy to perceived sensitivity of service accessed. Users created passwords that they considered more secure when they perceived the service to be sensitive. Further, the modelling interviews indicated all groups were more prepared to follow stricter security policies for sensitive services. Importantly, this depends on the perception of the user – services considered sensitive by an organization may not be considered sensitive by users.

4. Incorporate security within the task or job role. The modelling indicated the Computer Scientist group were more willing to expend effort to create secure passwords and a crucial part of this willingness was the integration of security within

their job role or their task. Encouraging other users to be more like computer scientists is not a new idea within the security literature but our contribution is to emphasise the importance of treating security as part of the task (or job) rather than a hindrance to task performance. Thus, alterations to the interface or task design that integrate password entry within the primary task could increase user motivation to generate secure passwords. For example, information that is sensitive but not meaningful to the user could be integrated within more meaningful tasks that are password protected.

5. Consider user motivation before imposing security demands. The task modelling found that unmotivated users simply ignored some security policies (i.e. creating unique passwords for every account). Imposing demands on unwilling users can be counterproductive as they will simply devise workarounds. This echoes the findings of Beautement and Sasse (2009) and suggests security officers should consider compliance with previous policies as a guide to user motivation.

6. Emphasize the dangers of password reuse. As in other studies (i.e. Florencio and Herley, 2007), password reuse was a significant issue and quantitative analyses combined with modelling indicated that users' knowledge affected the extent of password reuse. The modelling interviews found that when users inferred the value of following guidelines for themselves compliance was greater. This is consistent with the literature on behaviour change and techniques such as motivational interviewing (Miller and Rollnick, 2002) could be used to impart knowledge and support user-initiated change rather than introducing top-down directives.

These recommendations are flexible and rely on the expertise of the security officer implementing them. For example, where users have low previous compliance indicating low motivation but are accessing a very sensitive service then recommendations 3 and 5 make opposing predictions. Nonetheless, our results show that this reflects the reality of password use outside the laboratory. In these instances security officers must use their knowledge of the current situation combined with their previous experience. One value of this research is to signpost those variables that are likely to be important in different situations and to encourage security officers to engage with multiple factors and the interactions between them.

7.3. Limitations and Future Research

As noted in Section 4 the sample size of the dataset was not large and this limits the generalizability of the findings reported here. However, given the lack of models of password behaviour, our aim was to produce a first step in capturing some of the detail of user behaviour across different groups. Smaller sample sizes and even case studies are often the richest source for theory development due to the detailed study these studies permit (Salkovskis, 2002). Here the approach has enabled the identification of constraints and generated hypotheses about the way these constraints interact. Nonetheless, having constructed these models there is now a need to validate and develop them using larger sample sizes and further studies. The reliance on self-report measures means that we cannot eliminate the possibility of demand characteristics biasing their responses. Further studies could address this by including objective measures within task modelling, for example system logs of frequency of password entry. Another potential avenue is to construct an ideal model of password behaviour and contrast our models with this ideal to help identify gaps in password security that can be targeted through security policies.

Our models show that password behaviour is dependent on multiple constraints that operate simultaneously. When constraints are combined, less intuitive and more sophisticated predictions can be inferred. Here we have only considered simple combinations of constraints but our hope is that further studies and subsequent task modelling would represent more complex interactions between constraints. Another ambition for subsequent modelling work is to provide input to mathematical models (Collinson et al., 2009; 2010) to generate economic predictions for adopting specific password policies. Such comprehensive modelling would allow different policies to be devised and user behaviour to be compared for each policy.

A key advance for such modelling work would be the formal specification of a utility function for password behaviour. Our study showed the value of this as between group differences in goals were a key factor in explaining differences in password security. Users appear to trade-off gains in password security with costs in effort and time spent maintaining passwords. Because these trade-offs occur within different

internal and external constraints across passwords it is necessary to study all of these factors and the way that they interact to predict password behaviour. The models described here are a first attempt at this task.

Acknowledgements

This work was supported by grant P0007E ("Trust Economics") from the UK Technology Strategy Board (TSB). We would like to thank members of the Trust Economics team (www.trust-economics.org) for their input and Jens Riegelsberger and three anonymous reviewers for their comments on an earlier version of this manuscript.

References

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*, 26-33.

Allen, R. B., 1990. User models: Theory, method, and practice. *International Journal of Man-Machine Studies, 32*, 511-543.

Anderson, J.R., 1990. *Rational Analysis*. Hillsdale, NJ: Erlbaum.

Anderson, J. R., Schooler, L. J., 2001. Reflections of environment in memory. *Psychological Science, 2(6),* 396-408.

Anderson, R., 2001. Why Information Security is Hard – An economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference, ACSAC '01*, New Orleans, USA, 10-14.

Baldwin, A., Beres, Y., Duggan, G. B., Cassa Mont, M., Johnson, H., Middup, C., Shiu, S. (2011). Economic methods and decision making by security professionals. *Proceedings of the Tenth Workshop on Economics and Information Security, WEIS 2011*. Fairfax, USA.

Beautement, A., and Sasse, M. A., 2009. The economics of user effort in information security. *Computer Fraud & Security, 10*, 8-12.

Bonneau, J., and Preibusch, S., 2010. The password thicket: technical and market failures in human authentication on the web. *Proceedings of the Ninth Workshop on Economics and Information Security, WEIS 2010.* London, UK.

Browne, G. J., Pitts, M. G., 2004. Stopping rule use during information search in design problems, *Organizational Behavior and Human Decision Processes, 95,* 208-224.

Carter, S., Mankoff, J. (2005). When participants do the capturing: The role of media in diary studies. *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 899-908.

Cohen, J. D., McClure, S. M., Yu, A. J., 2007. Should I stay or should I go? How the human brain manages the trade-off between exploitation and exploration. *Philosophical Transactions of the Royal Society B: Biological Sciences, 362*, 933-942.

Collinson, M., Monahan, B., Pym, D. (2009). A logical and computational theory of located resource. *Journal of Logic and Computation, 19,* 1207-1244.

Collinson, M., Monahan, B., Pym, D. (2010). Semantics for structured systems modelling and simulation. *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques*, Torremolinos, Spain.

Cranor, L. F., 2008. A framework for reasoning about the human in the loop. *Proceedings of the 1st Conference on Usability, Psychology and Security*.

Ebbinghaus, H., 1964, 1885. *Memory: A contribution to experimental psychology*. Meneola, NY: Dover Publications.

Ericsson, K. A., Polson, P. G., 1988. An experimental analysis of a memory skill for dinner-orders. *Journal of Experimental Psychology: Learning, Memory and Cognition, 14*, 305-316.

Fischer, G., 2001. User modeling in human-computer interaction. *Journal of User Modeling and User-Adapted Interaction, 11*, 65-86.

Florencio, D., Herley, C., 2007. A large scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, Banff, Alberta, Canada, 657-666.

Florencio, D., Herley, C., 2010. Where do security policies come from? *Symposium On Usable Privacy and Security, SOUPS '10*, Redmond, USA.

Gaw, S., Felten, E. W., 2006. Password management strategies for online accounts. *Symposium On Usable Privacy and Security, SOUPS '06*, Pittsburgh, USA, 44-55.

Grawemeyer, B., Johnson, H., 2011. Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*, 256-267.

Herley, C., 2009. So long and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the New Security Paradigms Workshop, NSPW '09*. Oxford, UK.

Hoonakker, P., Bornoe, N., Carayon, P., 2009. Password authentication from a human factors perspective: Results of a survey among end-users. *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting*, San Antonio, USA, 459-463.

Howes, A. Lewis, R.L., Vera, A., 2009. Rational adaptation under task and processing constraints: Implications for testing theories of cognition and action. *Psychological Review, 116*, 4, 717-751.

Inglesant, P., Sasse, M. A., 2010. The true cost of unusable password policies: Password use in the wild. *Proceedings of the ACM Conference on Human Factors in Computing Systems, CHI '10*. Atlanta, USA, 382-392.

Ives, B., Walsh, K. R., Schneider, H., 2004. The domino effect of password reuse. *Communications of the ACM, 47(4),* 75-78.

Jensen, C., Potts, C., Jensen, C., 2005. Privacy practices of Internet users: Self reports versus observed behavior. *International Journal of Human-Computer Studies, 63,* 203-227.

Johnson, H., Hyde, J. (2003). Towards modeling individual and collaborative construction of jigsaws using task knowledge structures (TKS). *ACM Transactions on Computer-Human Interaction, 10,* 339-387.

Johnson, H., Johnson, P., 1989. Integrating task analysis into system design surveying designers needs. *Ergonomics, 32,* 1451-1467.

Kahneman, D., 2003. A perspective on judgement and choice: Mapping bounded rationality, *American Psychologist, 58,* 697-720.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., 2011. Of passwords and people: Measuring the effect of password-composition policies. *Proceedings of the ACM Conference on Human Factors in Computing Systems, CHI '11*. Vancouver, Canada, 2595-2604.

Keith, M., Shao, B., Steinbart, P. J., 2007. The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65,* 17-28.

McCrickard, D. S., Chewar, C. M., Somervell, J. P., Ndiwalana, A., 2003. A model for notification systems evaluation – assessing user goals for multitasking activity. *ACM Transactions on Computer-Human Interaction, 10,* 312-338.

Miller, W. R., Rollnick, S., 2002. *Motivational interviewing: Preparing people for change* (2nd ed.). New York: Guilford Press.

Muth, J. F., 1961. Rational expectations and the theory of price movements. *Econometrica, 29,* 315-335.

O'Neill, E. J., Johnson, P., Johnson, H., 1999. Representations and user-developer interaction in cooperative analysis and design. *Human-Computer Interaction, 14, 1and2,* 43–91.

Pawson, R., Tilley, N., 1997. Realistic Evaluation. London: Sage.

Parkin, S., van Moorsel, A., Inglesant, P., Sasse, M. A., 2010. A stealth approach to usable security: Helping IT security managers to identify workable security solutions. *Proceedings of the New Security Paradigms Workshop, NSPW '10*. Concord, USA.

Payne, S. J., Duggan, G. B., Neth, H., 2007. Discretionary task interleaving: Heuristics for time allocation in cognitive foraging. *Journal of Experimental Psychology: General, 136*, 370-388.

Rieman, J., 1993. The diary study: A work-place-oriented research tool to guide laboratory efforts. *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 321-326.

Salkovskis, P. M., 2002. Empirically grounded clinical interventions: Cognitive-behavioural therapy progresses through a multi-dimensional approach to clinical science. *Behavioural and Cognitive Psychotherapy, 30*, 3-9.

Sasse, M. A., Brostoff, S., Weirich, D., 2001. Transforming the "weakest link": a human-computer interaction approach to usable and effective security. *BT Technical Journal, 19(3*), 122-131.

Schneier, B., 2000. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley and Sons.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., 2010. Encountering stronger password requirements: User attitudes and behaviors. *Symposium On Usable Privacy and Security, SOUPS '10*, Redmond, USA.

Simon, H. A., 1957. *Models of man.* New York: Wiley.

Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *Proceedings of ACM Conference of Electronic Commerce, EC '01*, 38-47.

Vu, K., L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B., Cook, J., Schultz, E. E., 2007. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*, 744-757.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N., 2005. PassPoints: Design and longtitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies, 63*, 102-127.

Wild, P. J., Johnson, P., Johnson, H., 2004. Towards a composite modelling approach for multitasking. *3rd International Workshop on Task Models and Diagrams for User Interface Design, TAMODIA '04*, 17-24, Prague, Czech Republic.

Wogalter, M. S., 2006. Communication-human information processing (C-HIP) model. In M. S. Wogalter ed., *Handbook of Warnings*, Lawrence Erlbaum Associates, Mahwah, New Jersey.

Yan, J., Blackwell, A., Anderson, R., Grant, A., 2004. Password memorability and security: empirical results. *IEEE Security and Privacy, 2*, 25-31.

Zviran, M., Haga, W. J., 1999. Password security: An empirical study. *Journal of Management Information Systems, 15*, 161-185.

Figure Captions

Figure 1. Correlation between rated sensitivity of task and estimated security of the corresponding password in all three user groups. Larger data points denote more than one password with the same value ranging from smallest (1 password) to largest (12 passwords).

Figure 2. Correlation between estimated security and frequency of usage for each password in all three user groups. Larger data points denote more than one password with the same value ranging from smallest (1 password) to largest (11 passwords).

Figure 3. Mean perceived task sensitivity for unique and reused passwords in all three user groups. Error bars are standard errors.

Figure 4. Mean frequency of use for unique and reused passwords in all three user groups. Error bars are standard errors.

Figure 5. Task Knowledge Structure (TKS) for password creation and use for an individual user in the Admin group.

Figure 6. Task Knowledge Structure (TKS) for password creation and use for the Admin group.

Figure 7. Task Knowledge Structure (TKS) for password creation and use for the Student group.

Figure 8. Task Knowledge Structure (TKS) for password creation and use for the Computer Scientist group.

	Comp. Scientist	Student	Admin
Single word/name	.20	.06	.63
Meaningful phrase	0	.14	.06
Abbreviation meaningful phrase	.43	.25	.17
Meaningful letters and numbers	.11	.06	0
Number pattern	.11	.01	.11
Random	.09	.17	0
Other pattern	.06	.28	.03

Table 1. Proportion of different password types in each of the three user groups.

User Motivation	General Knowledge	Task Knowledge	
		Taxonomic structure	Goal structure
Attitude towards company Status within company Personal characteristics, e.g. laziness	Awareness of threats and likelihood of attacks Knowledge of previous security policy and breaches Accountability of security breach Personal and company security history	Password elements: -Length -Type of characters, i.e. letters, numbers, symbols -Structure, i.e. words from a dictionary, capitalization Composition of user ID Relationship between password and user ID Reason for password Factors that affect security of password Other passwords in use Relationship to other passwords in use	Strategies -Reuse all of password -Reuse part of password -Offload to environment -Share with others

Table 2. Constraints internal to the user that affect password security

Organisation	Environment	Task
Culture of organisation	Job role – responsibilities and level of control	Importance of task
General security policy including after breaches	Social aspects of relationships with colleagues	Frequency of task execution
Specific password policy	Time pressure	Extent of interleaving with other tasks
Clarity and availability of rules	Location	Type of task – work or leisure
Extent to which rules are enforced or voluntarily applied	Resources available	Availability of alternative tasks
	Extent of collaboration and interdependencies with others	Tasks completed before and after current task
		Number of similar tasks requiring passwords

Table 3. Constraints external to the user that affect password security

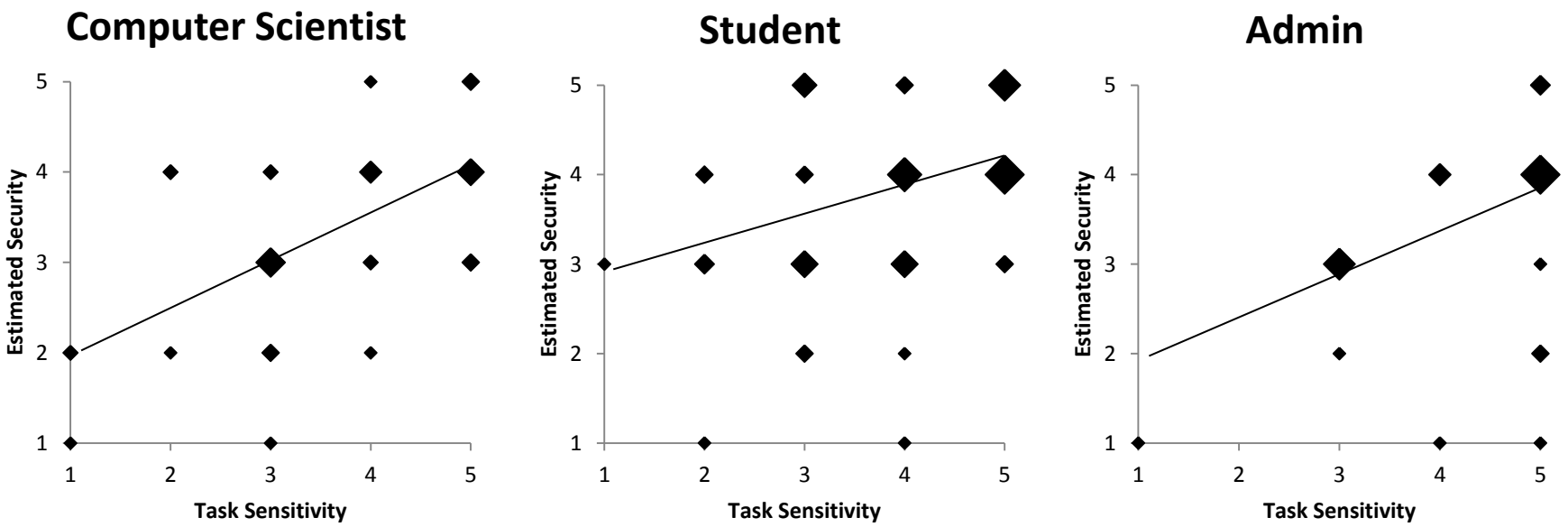


Figure 1. Correlation between rated sensitivity of task and estimated security of the corresponding password in all three user groups. Larger data points denote more than one password with the same value ranging from smallest (1 password) to largest (12 passwords).

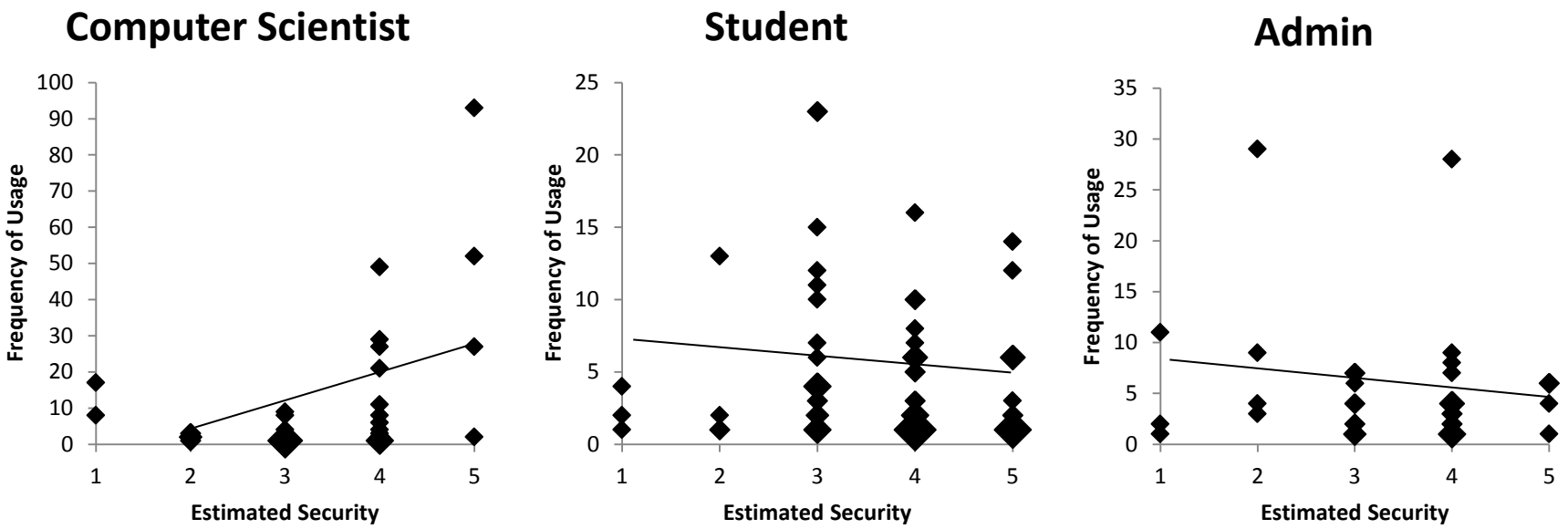


Figure 2. Correlation between estimated security and frequency of usage for each password in all three user groups. Larger data points denote more than one password with the same value ranging from smallest (1 password) to largest (11 passwords).

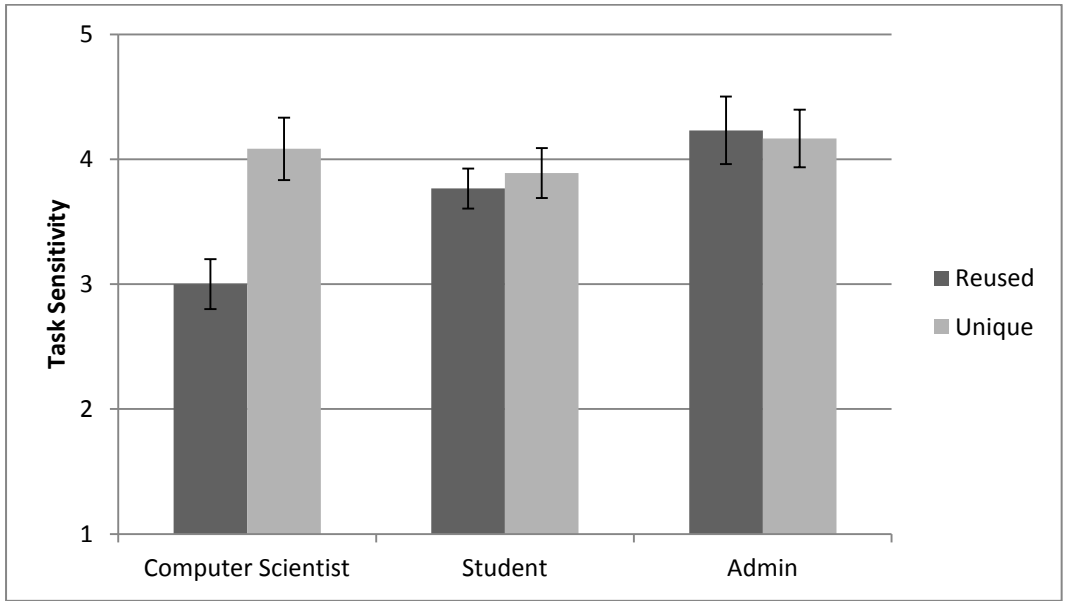


Figure 3. Mean task sensitivity for unique and reused passwords in all three user groups. Error bars are standard errors.

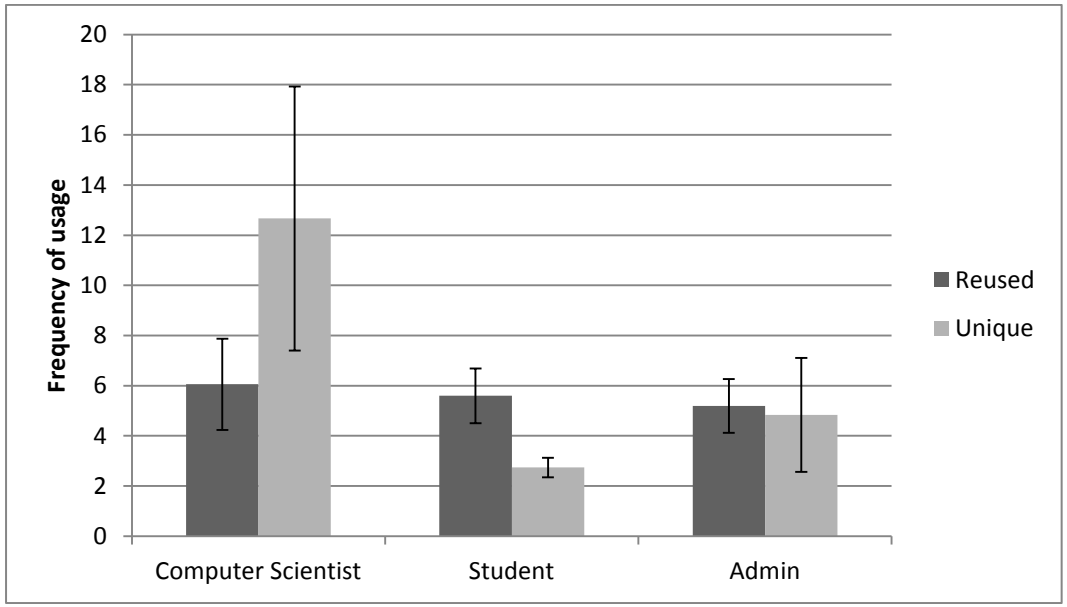


Figure 4. Mean frequency of use for unique and reused passwords in all three user groups. Error bars are standard errors.

Figure 5

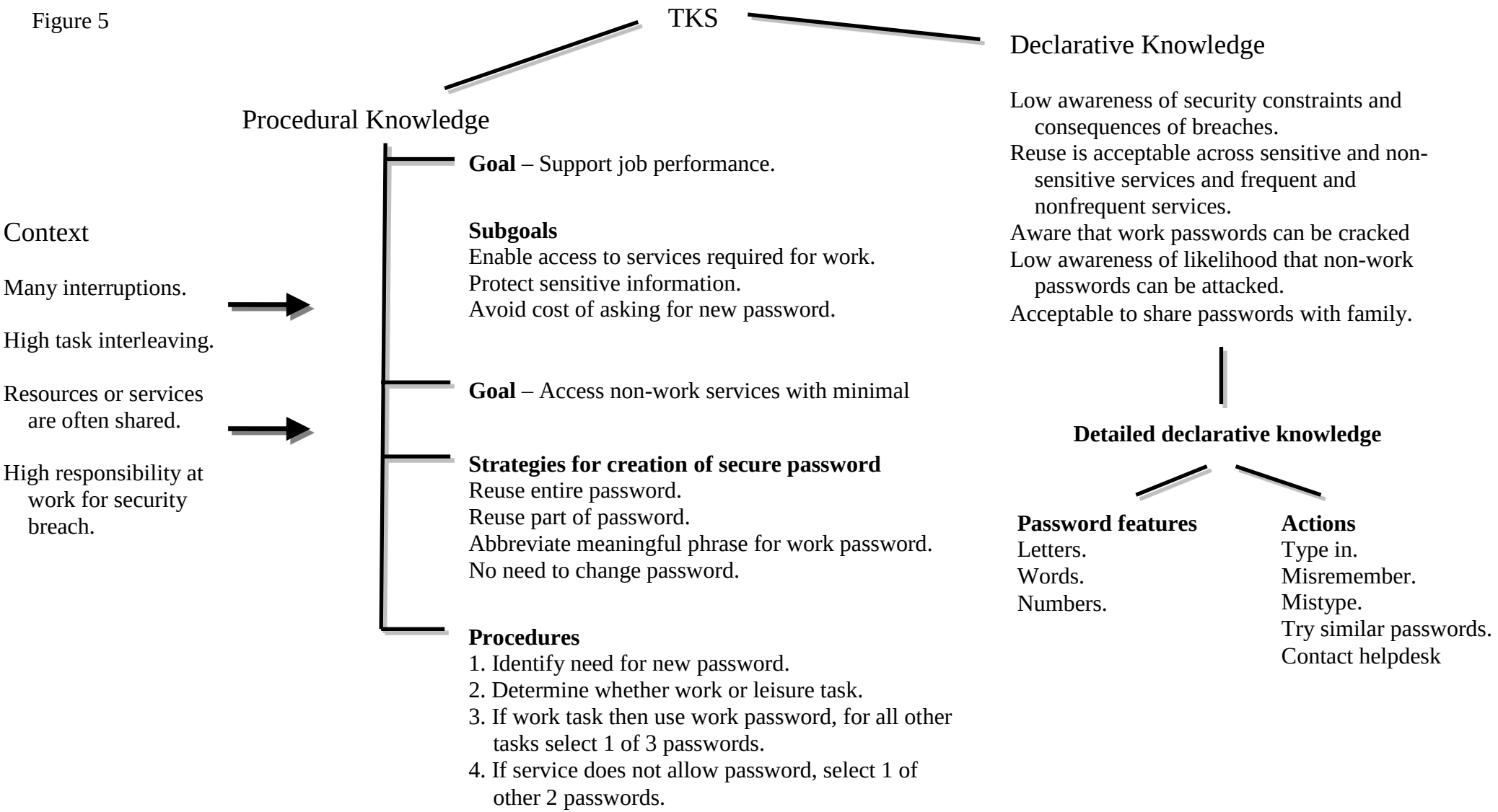

TKS
Declarative Knowledge
Low awareness of security constraints and consequences of breaches.
Reuse is acceptable across sensitive and non-sensitive services and frequent and nonfrequent services.
Aware that work passwords can be cracked
Low awareness of likelihood that non-work passwords can be attacked.
Acceptable to share passwords with family.
Detailed declarative knowledge
Password features
Letters.
Words.
Numbers.
Actions
Type in.
Misremember.
Mistype.
Try similar passwords.
Contact helpdesk
Procedural Knowledge
Goal – Support job performance.
Subgoals
Enable access to services required for work.
Protect sensitive information.
Avoid cost of asking for new password.
Goal – Access non-work services with minimal
Strategies for creation of secure password
Reuse entire password.
Reuse part of password.
Abbreviate meaningful phrase for work password.
No need to change password.
Procedures
1. Identify need for new password.
2. Determine whether work or leisure task.
3. If work task then use work password, for all other tasks select 1 of 3 passwords.
4. If service does not allow password, select 1 of other 2 passwords.
Context
Many interruptions.
High task interleaving.
Resources or services are often shared.
High responsibility at work for security breach.

Figure 6

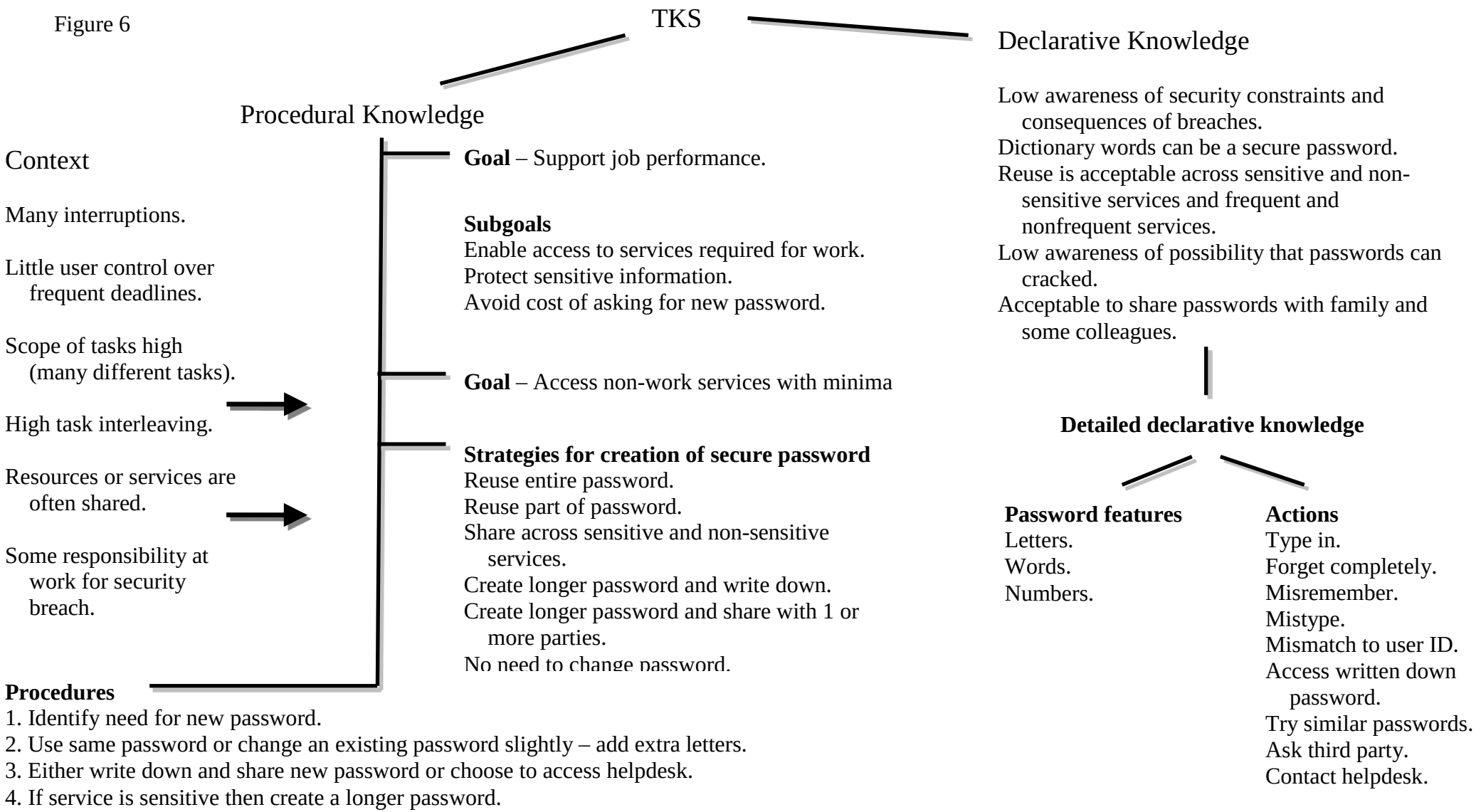

TKS
Declarative Knowledge
Low awareness of security constraints and consequences of breaches.
Dictionary words can be a secure password.
Reuse is acceptable across sensitive and non-sensitive services and frequent and nonfrequent services.
Low awareness of possibility that passwords can cracked.
Acceptable to share passwords with family and some colleagues.
Detailed declarative knowledge
Password features
Letters.
Words.
Numbers.
Actions
Type in.
Forget completely.
Misremember.
Mistype.
Mismatch to user ID.
Access written down password.
Try similar passwords.
Ask third party.
Contact helpdesk.
Procedural Knowledge
Context
Many interruptions.
Little user control over frequent deadlines.
Scope of tasks high (many different tasks).
High task interleaving.
Resources or services are often shared.
Some responsibility at work for security breach.
Goal – Support job performance.
Subgoals
Enable access to services required for work.
Protect sensitive information.
Avoid cost of asking for new password.
Goal – Access non-work services with minima
Strategies for creation of secure password
Reuse entire password.
Reuse part of password.
Share across sensitive and non-sensitive services.
Create longer password and write down.
Create longer password and share with 1 or more parties.
No need to change password.
Procedures
1. Identify need for new password.
2. Use same password or change an existing password slightly – add extra letters.
3. Either write down and share new password or choose to access helpdesk.
4. If service is sensitive then create a longer password.

Figure 7

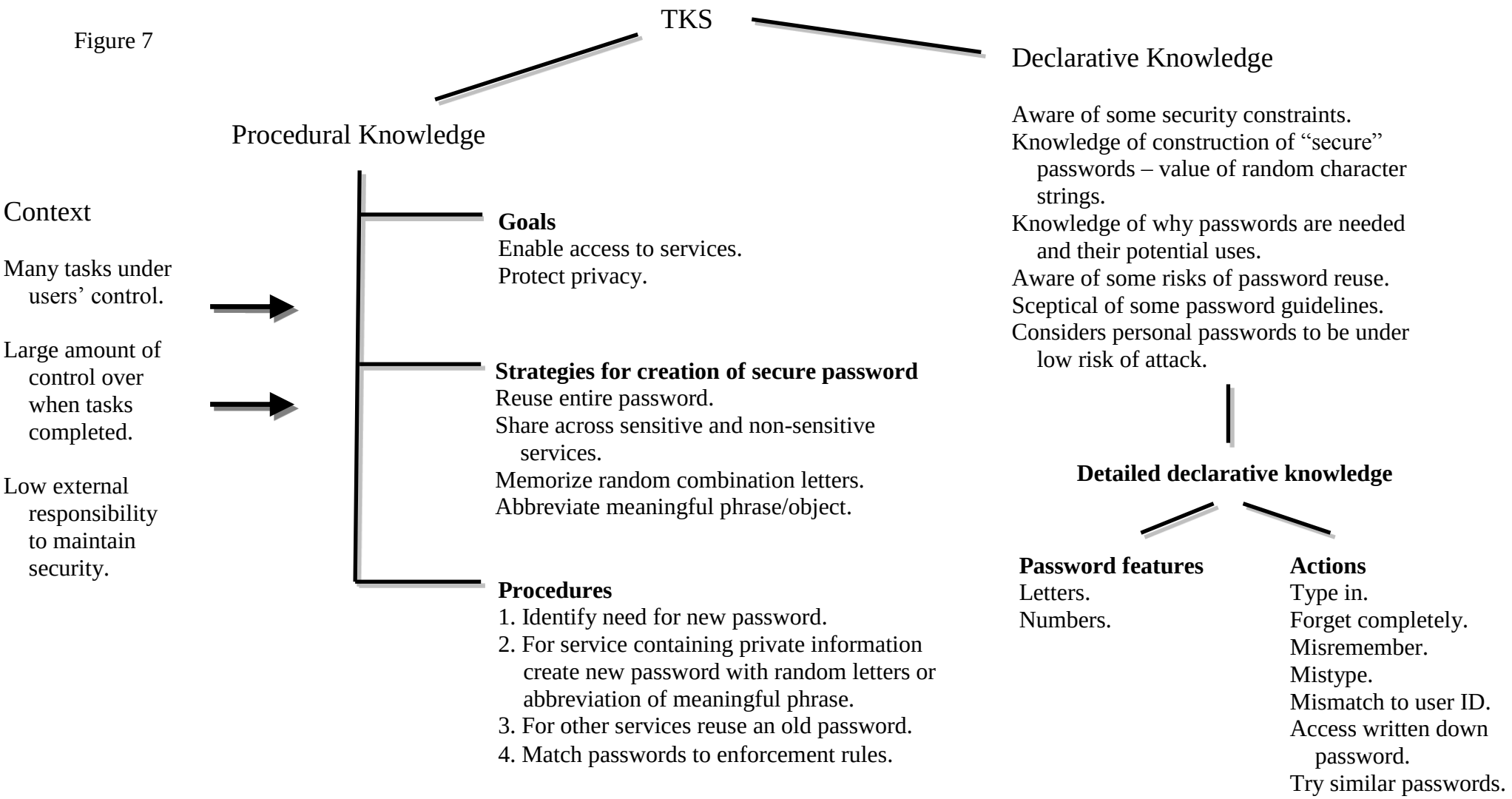
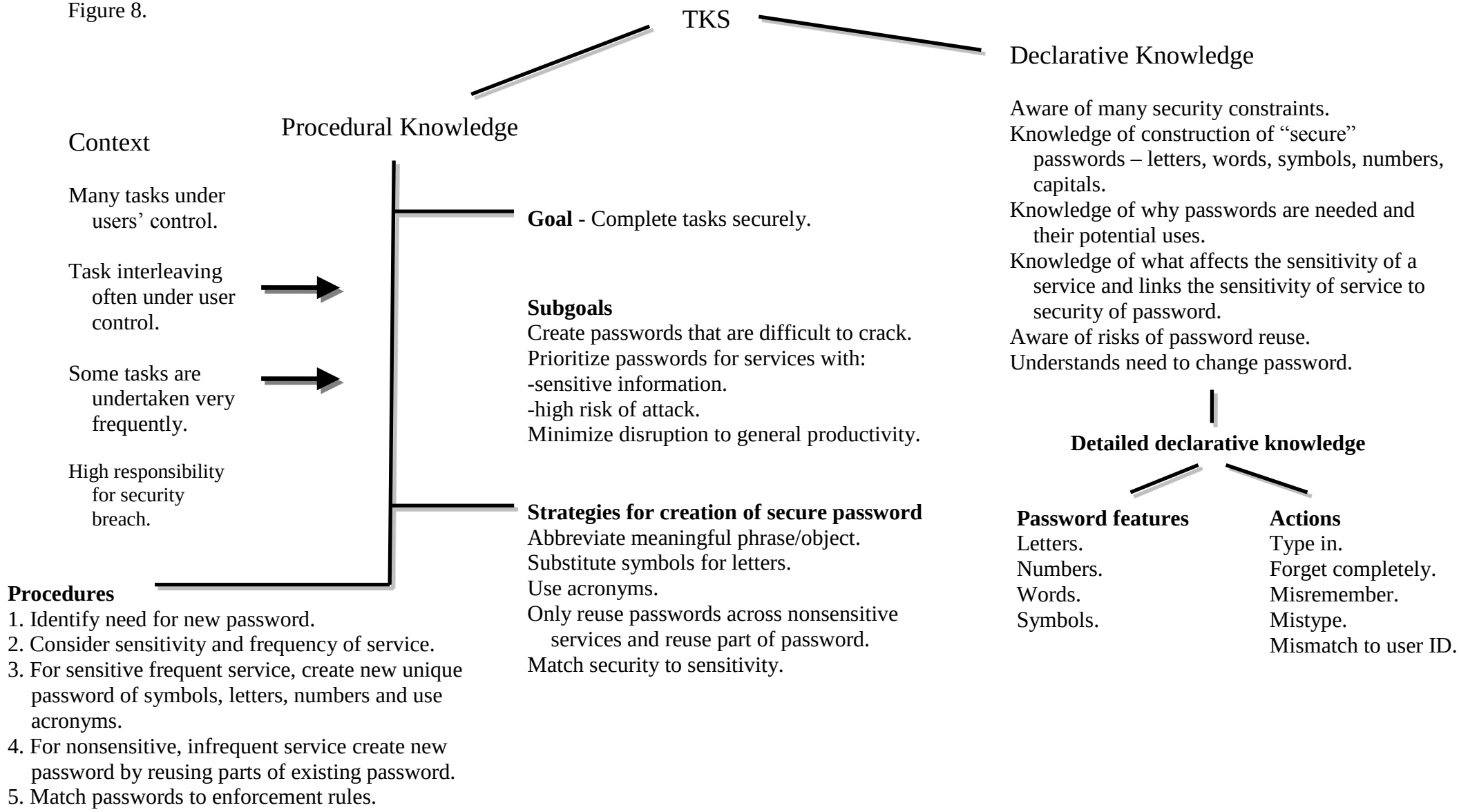

TKS
Declarative Knowledge
Aware of some security constraints.
Knowledge of construction of "secure" passwords – value of random character strings.
Knowledge of why passwords are needed and their potential uses.
Aware of some risks of password reuse.
Sceptical of some password guidelines.
Considers personal passwords to be under low risk of attack.
Detailed declarative knowledge
Password features
Letters.
Numbers.
Actions
Type in.
Forget completely.
Misremember.
Mistype.
Mismatch to user ID.
Access written down password.
Try similar passwords.
Procedural Knowledge
Context
Many tasks under users' control.
Large amount of control over when tasks completed.
Low external responsibility to maintain security.
Goals
Enable access to services.
Protect privacy.
Strategies for creation of secure password
Reuse entire password.
Share across sensitive and non-sensitive services.
Memorize random combination letters.
Abbreviate meaningful phrase/object.
Procedures
1. Identify need for new password.
2. For service containing private information create new password with random letters or abbreviation of meaningful phrase.
3. For other services reuse an old password.
4. Match passwords to enforcement rules.

Figure 8.


TKS
Declarative Knowledge
Aware of many security constraints.
Knowledge of construction of "secure" passwords – letters, words, symbols, numbers, capitals.
Knowledge of why passwords are needed and their potential uses.
Knowledge of what affects the sensitivity of a service and links the sensitivity of service to security of password.
Aware of risks of password reuse.
Understands need to change password.
Detailed declarative knowledge
Password features
Letters.
Numbers.
Words.
Symbols.
Actions
Type in.
Forget completely.
Misremember.
Mistype.
Mismatch to user ID.
Procedural Knowledge
Context
Many tasks under users' control.
Task interleaving often under user control.
Some tasks are undertaken very frequently.
High responsibility for security breach.
Goal - Complete tasks securely.
Subgoals
Create passwords that are difficult to crack.
Prioritize passwords for services with:
-sensitive information.
-high risk of attack.
Minimize disruption to general productivity.
Strategies for creation of secure password
Abbreviate meaningful phrase/object.
Substitute symbols for letters.
Use acronyms.
Only reuse passwords across nonsensitive services and reuse part of password.
Match security to sensitivity.
Procedures
1. Identify need for new password.
2. Consider sensitivity and frequency of service.
3. For sensitive frequent service, create new unique password of symbols, letters, numbers and use acronyms.
4. For nonsensitive, infrequent service create new password by reusing parts of existing password.
5. Match passwords to enforcement rules.